DOCKET FILE COPY ORIGINAL

ORIGINAL

BEFORE THE

Federal Communications Commission

WASHINGTON, DC 20554

In the Matter of:	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	
	)	

COMMENTS OF PRIMECO PERSONAL COMMUNICATIONS, L.P.

PRIMECO PERSONAL COMMUNICATIONS, L.P.

William L. Roughton, Jr.
Associate General Counsel
601 13th Street, N.W. Suite 320 South
Washington, D.C. 20005
(202) 628-7735

Its Attorney

May 20, 1998

TABLE OF CONTENTS

SUMMARY

Since enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, privacy laws have protected the privacy of electronic communications by affirmatively limiting law enforcement's electronic surveillance activities. CALEA affirms those privacy protections, and while Congress imposed compliance burdens on carriers, it also sought to minimize the costs of CALEA compliance to carriers and consumers.

In reviewing the FBI/DOJ Petition, CALEA requires the Commission to balance three important objectives: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies. To achieve this balance, the Commission is required by statute to preserve the *status quo* with respect to information available to law enforcement, and to affirm the cost- and technology-based limits on the capabilities that law enforcement may seek of carriers. Congress intended that industry have the primary role in standards development, and industry's standard is presumptively CALEA-compliant unless a petitioner affirmatively demonstrates that the standard is "deficient" and does not meet CALEA's capability requirements.

FBI/DOJ have failed to demonstrate that the industry standard is deficient. FBI/DOJ's requested capabilities and features all are beyond the scope of the capability assistance requirements enumerated in CALEA. Thus, the FBI/DOJ Petition should be rejected.

While the industry standard satisfies CALEA's capability requirements, *if* modifications are deemed necessary, the standard should be remanded to industry for development and implementation of the necessary standards work. Lastly, FBI/DOJ's request that the Commission make new standards effective 18 months from the Commission's decision in this proceeding should be rejected. 18 months is an insufficient time period for industry to develop standards, for manufacturers to design and test modifications, and for carriers to implement and test the modifications.

BEFORE THE

Federal Communications Commission

WASHINGTON, DC 20554

In the Matter of:	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	
	)	

COMMENTS OF PRIMECO PERSONAL COMMUNICATIONS, L.P.

PrimeCo Personal Communications, L.P. ("PrimeCo")[1] hereby submits comments in response to the Commission's Public Notice of April 20, 1998 regarding issues raised in petitions for rulemaking concerning the scope of assistance capability requirements necessary to satisfy telecommunications carriers' obligations under the Communications Assistance for Law Enforcement Act ("CALEA").[2] As discussed herein, a reading of CALEA's statutory provisions and its legislative history, considered together with existing privacy laws, demonstrate that the FBI/DOJ "punch list" features fall outside CALEA's scope and should not be mandated. In addition, in the event the Commission determines changes are needed, it should remand such work to industry standards-setting bodies for development and deployment purposes.

---

1 PrimeCo is the broadband A/B Block PCS licensee or is the general partner/majority owner in the licensee in the following MTAs: Chicago, Milwaukee, Richmond-Norfolk, Dallas-Fort Worth, San Antonio, Houston, New Orleans-Baton Rouge, Jacksonville, Tampa-St. Petersburg-Orlando, Miami and Honolulu.

2 *In the Matter of: Communications Assistance for Law Enforcement Act, Public Notice*, CC Docket No. 97-213, DA 98-762 (released April 20, 1998) at 3 ("Public Notice").

DISCUSSION

I. BACKGROUND

As discussed below, privacy laws and CALEA together affirmatively limit law enforcement's electronic surveillance activities and the capabilities law enforcement may demand of carriers. Such limits are imposed for two primary purposes: (1) privacy protections, and (2) to minimize the costs of CALEA compliance to carriers and consumers. The Commission must evaluate the petition filed by the Federal Bureau of Investigation and U.S. Department of Justice ("FBI/DOJ Petition"), as well as petitions filed by other parties, against this statutory backdrop.[3]

A. CALEA Expressly Preserves Existing Privacy Laws and Imposes Additional Restrictions on Law Enforcement

The Commission appropriately requests that commenters address the relevance of existing privacy laws and their legislative history to CALEA's capability standards. In evaluating FBI/DOJ requested capabilities, the Commission must remember that CALEA's capability provisions were not enacted in a legislative vacuum and that, for 25 years prior to CALEA and continuing to the present time, privacy laws have acted as an affirmative restraint on law enforcement electronic surveillance activities.

---

[3] *See* Federal Bureau of Investigation and U.S. Department of Justice, Joint Petition for Expedited Rulemaking, CC Docket No. 97-213, filed March 27, 1998 ("FBI/DOJ Petition"); Center for Democracy and Technology, Petition for Rulemaking, CC Docket No. 97-213, filed March 26, 1998 ("CDT Petition"); Cellular Telecommunications Industry Ass'n, Petition for Rulemaking, CC Docket No. 97-213, filed July 16, 1997 ("CTIA Petition"). The Commission also seeks comment on an FBI/DOJ motion to dismiss CTIA's petition. Public Notice at 4-5; FBI/DOJ Joint Motion to Dismiss CTIA's July 16, 1997 Petition for Rulemaking, CC Docket No. 97-213, filed March 27, 1998 ("FBI/DOJ Motion").

CALEA simply supplements existing privacy laws while preserving law enforcement's limited wiretap authority and capabilities.

As the House Judiciary Committee noted in CALEA's legislative history, electronic surveillance by law enforcement has been governed since 1968 by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").[4] It should be emphasized that Title III was *not* enacted to give law enforcement agencies the ability or authority to conduct electronic surveillance; prior to the 1968 Act, law enforcement *already* was conducting wiretaps subject primarily to state law and constitutional considerations.[5] Rather, Title III was adopted in response to the Supreme Court's decisions in *Berger v. New York* and *Katz v. United States* to *limit* the circumstances under which a court may authorize such surveillance.[6] Title III's legislative history explained that the 1968 Act "has at its dual purpose (1) protecting the privacy of wire and oral communications and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be

---

4 *See* H.R. Rep. No. 103-827, at 11 (1994) ("House Report") (citing Pub. L. No. 90-351, Title III, 82 Stat. 112 (1968)); *see also id.* at 20 (CALEA's capability requirements "are *in addition to* the existing necessary assistance requirements" of Title 18, Section 2518(4)) (emphasis added).

5 *See* S. Rep. No. 90-1097 (1968) ("1968 Report"), reprinted at 1968 U.S.C.C.A.N. 2112, 2153.

6 *See id.* (citing *Berger*, 388 U.S. 41 (1967), and *Katz*, 389 U.S. 347 (1967)); *id.* 1968 U.S.C.C.A.N. at 2163 ("[w]orking from the hypothesis that any wiretapping and electronic surveillance should include the [*Berger* and *Katz*] constitutional standards, the subcommittee has used the *Berger* and *Katz* decisions as a guide in drafting Title III").

authorized."[7] The Supreme Court has further affirmed that in enacting Title III "the protection of privacy was an overriding congressional concern."[8]

CALEA's capability requirements did not tilt this balance in favor of law enforcement. In fact, in deliberating over CALEA, the Judiciary Committee "concluded that continued change in the telecommunications industry deserves legislative attention to *preserve* the balance sought in 1968 and 1986."[9] Indeed, Congress limited the capabilities that law enforcement may demand of carriers in large part to address privacy concerns.[10] As discussed below, moreover, the Judiciary Committee also concluded "that a *third concern* now explicitly had to be added to the balance, namely, the goal of ensuring that the telecommunications industry was not hindered in the rapid development and deployment of the new services and technologies that continue to benefit and revolutionize society."[11] Thus, Title III continues to act as a restraint on law enforcement after CALEA's enactment and CALEA itself, while imposing a new compliance obligation on carriers, also imposed its own restraint on law enforcement. The FBI/DOJ

---

7 *See* 1968 Report, 1968 U.S.C.C.A.N. at 2153. Congress expressly extended the privacy protections and limited law enforcement intercept authority of Title III to wireless technologies in 1986. *See* Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1851 (1986) (codified in relevant part at 18 U.S.C. § 2510(10)).

8 *Gelbard v. United States*, 408 U.S. 41, 48 (1972); *see also Lam Lek Chong v. U.S. Drug Enforcement Admin.*, 929 F.2d 729, 732-33 (D.C. Cir. 1991); *United States v. Lyons*, 507 F. Supp. 551, 553-54 (D. Md. 1981), *aff'd*, 695 F.2d 802 (4th Cir. 1982).

9 House Report at 13 (emphasis added).

10 *See id.* at 17-18.

11 *Id.* at 12-13 (emphasis added).

Petition must therefore be viewed in the context of (1) Title III's and CALEA's protection of privacy interests, and (2) CALEA's protection of services and technology development and deployment.

B. CALEA Requires Independent Commission Review to Determine Whether Petitioners Have Demonstrated the Industry's Standard is Deficient

At the time CALEA was enacted, carriers acknowledged that new wireless technologies and advanced calling features have made authorized government surveillance activities more difficult to conduct.[12] While also recognizing these developments, Congress nevertheless sought to "balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."[13] CALEA achieves this balance by *preserving* the *status quo* with respect to information available to law enforcement, and by imposing cost- and technology-based limits on the capabilities that law enforcement may demand of carriers.

CALEA enumerates specific assistance capability requirements for telecommunications carriers.[14] In enacting these requirements, Congress expressly stated its intent *not* to expand the information to which law enforcement is entitled, and that all

---

12 *See id.* at 15-16.

13 *Id.* at 13.

14 *See* 47 U.S.C. § 1002.

parties — the Commission, law enforcement and industry — are to narrowly interpret capability assistance obligations. The House Judiciary Committee stated that:

> The Committee intends the assistance requirements . . . to be both *a floor and a ceiling*. The FBI Director testified that the legislation was intended *to preserve the status quo*, that it was intended to provide law enforcement *no more and no less access to information than it had in the past*. The Committee urges *against overbroad interpretation* of the requirements. The legislation gives industry, in consultation with law enforcement and subject to review by the FCC, a key role in developing the technical requirements and standards that will allow implementation of the requirements. The Committee expects industry, law enforcement and the FCC to *narrowly interpret* the requirements.[15]

This balance is further reflected in CALEA's mechanism for establishing standards. Law enforcement is given a consultative role, which industry has fully accommodated. CALEA by its plain terms, however, leaves the standards-setting process to industry associations or standard-setting organizations, a policy confirmed by its legislative history.[16] Moreover, if a government agency or any other person believes that the standards are deficient, that agency or person may petition *the Commission* to establish by rule, technical requirements that:

- meet CALEA's assistance capability requirements by *cost-effective methods*;

---

15 House Report at 22-23 (emphasis added).

16 *See* 47 U.S.C. §§ 1006(a)-(b); House Report at 19 ("the telecommunications industry itself shall decide how to implement law enforcement's requirements . . . [and] allows industry associations and standard-setting bodies, in consultation with law enforcement to establish publicly available specifications creating 'safe harbors' for carriers."), 26-27 (discussing appropriateness of delegating authority to issue standards to private industry parties); *see also* 47 U.S.C. § 1002(b), House Report at 23 (law enforcement "not permitted to require the specific design of systems or features, nor prohibit adoption of any such design . . .").

- protect the *privacy and security* of communications *not authorized* to be intercepted;
- *minimize the cost* of such compliance on residential rate-payers;
- serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the carrier's assistance capability obligations during any transition period.[17]

Thus, Congress intended that industry have the primary role in standards development and, absent the filing of Section 107(b) deficiency petitions, industry's standard is presumptively consistent with CALEA.[18] Moreover, in the event of dispute, Congress mandated that the *Commission* determine whether the industry standard is CALEA-compliant.

The Commission must carefully review the FBI/DOJ Petition to determine whether petitioners have *affirmatively demonstrated* that the industry standard *does not meet* these requirements. Indeed, a Commission determination that the FBI's punch list items do not exceed CALEA's scope is *insufficient* to warrant a Commission finding that the industry standard is deficient. Finally, the five factors of Section 107(b) that the Commission must consider in reviewing the FBI/DOJ Petition involve considerations well within the Commission's expertise and, as Congress designated the Commission

---

17 47 U.S.C. § 1006(b).

18 *See id.* § 1006(a)(2) (carrier deemed in compliance with CALEA capability requirements if it "is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, *or* by the Commission under" the petition provisions of 47 U.S.C. § 1006(b)) (emphasis added).

alone responsible for reviewing standards petitions, no deference to the statutory interpretation of the FBI/DOJ is required.[19]

II. THE FBI/DOJ "PUNCH LIST" ITEMS EXCEED THE SCOPE OF CALEA AND EXISTING PRIVACY LAWS

On December 5, 1997, the Telecommunications Industry Association ("TIA") and Committee T1 announced the adoption and joint publication of an interim industry standard, J-STD-025 (the "J-Standard"). The FBI/DOJ subsequently filed a joint petition for rulemaking requesting that the Commission correct purported deficiencies in the J-Standard. The Center for Democracy in Technology ("CDT") also filed a deficiency petition contending that the J-Standard exceeds the scope of CALEA, and asking the Commission to reject the capabilities sought by FBI/DOJ.[20] Finally, TIA has requested that the Commission resolve the dispute and remand any necessary standardization work back to TIA.[21] PrimeCo's comments in this section primarily address the FBI/DOJ "punch list" items set forth in the FBI/DOJ Petition.[22] As discussed

---

19 *See id.* § 1006(b) (government agency "may petition *the Commission*" if it believes the industry standards are deficient — emphasis added); *see also American Federation of Gov't Employees, AFL-CIO, Local 3306 v. FLRA*, 2 F.3d 6, 10 (2d Cir. 1993) ("deference is accorded an agency only when construing a statute it is charged with administering"); *Professional Airways Systems Specializes v. FLRA*, 809 F.2d 855, 857 n.6 (D.C. Cir. 1987) (same); *Tsosie v. Califano*, 651 F.2d 719, 722 (10th Cir. 1981) (agency's construction not entitled to special deference to the extent it rests on the interpretation of another agency's statutes and regulations).

20 CDT Petition at 4, 7-12.

21 Telecommunications Industry Ass'n, Petition for Rulemaking, CC Docket No. 97-213, filed April 2, 1998, 11-12 ("TIA Petition").

22 PrimeCo does note its view that Commission consideration of the FBI/DOJ Joint

(continued...)

herein, FBI/DOJ have failed to meet their burden to demonstrate that the J-Standard is deficient under CALEA, and the Commission should accordingly affirm the J-Standard as CALEA-compliant.

A. Conference Call Capability — Punch List Item 1

The J-Standard permits law enforcement to intercept a conference call so long as the subject of a *court order*, or another person using the subject's phone, remains connected to the call. This requirement largely mirrors the language of Section 103(a)(1) of CALEA and is consistent with existing practice.[23] FBI/DOJ, however, contend that CALEA requires that law enforcement should be able to intercept conference calls "after the subject [of the court order] leaves the conversation, temporarily *or permanently*."[24] Title III, however, requires that a court order "identify the person, if known, whose communications are to be intercepted" and "the place where authority to intercept is to be intercepted."[25] PrimeCo submits that this requested "punch list" requirement would

---

22 (...continued)
Motion to dismiss the CTIA Petition constitutes an unnecessary use of Commission time and resources, as Commission resolution of the issues raised in the FBI/DOJ Petition will implicitly address the FBI/DOJ Joint Motion and the CTIA Petition.

23 *See* 47 U.S.C. § 1002(a)(1). The FBI/DOJ Petition cites the Section 103(b)(1) capability requirement as "expeditiously isolating and enabling the government *** to intercept *** all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier." FBI/DOJ Petition at 27, ¶ 46. Conspicuously omitted from the FBI/DOJ citation, however, is the statutory language requiring that such interception be made *"pursuant to a court order or other lawful authorization."* *See* 47 U.S.C. § 1002(a)(1) (emphasis added).

24 FBI/DOJ Petition at 32, ¶ 55, App. proposed rule 64.1708(a) (emphasis added).

25 *See* 18 U.S.C. §§ 2511, 2518(1)(b), (4)(a)(b).

significantly undermine the privacy interests protected in Title III and which CALEA expressly preserves.[26] Commission approval of this feature would also directly contravene the statutory requirement that standards "protect the privacy and security of communications not authorized to be intercepted."[27] Further, and as a threshold matter, this capability is not currently provided to law enforcement, and therefore contravenes Congress' intent that CALEA standards provide law enforcement "no more and no less access to information than it had in the past."[28]

Moreover, even assuming *arguendo* that this feature complies with Section 103(a), it is questionable whether the requirement is cost-effective, as required by Section 107(b)(1). In this regard, utilization of a conference bridge service, whereby a wiretap subject initiates the call but uses a conference bridge service offered by another carrier or service provider, renders this punch list feature futile. Moreover, a "meet-me-conference bridge" is outside the capability of PrimeCo's network and switching facilities; thus, PrimeCo would have no control over law enforcement's access to the wiretap subject even if this feature were built into the switch. It is PrimeCo's understanding that development of this feature will be very costly and, regardless of the exact dollar figures, the futility of this requested feature alone renders it not cost-effective.

B. Additional "Call-Identifying" Information

Section 103(a)(2) requires that carriers must be capable of "expeditiously isolating and enabling the government, pursuant to a court order or other lawful

---

[26] *See* discussion of Title III *supra*.

[27] *See* 47 U.S.C. § 1006(b)(2).

[28] *See* House Report at 22-23.

authorization, to access call-identifying information that is reasonably available to the carrier — (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and (B) in a manner that allows it to be associated with the communication to which it pertains . . . ."[29] Call-identifying information, in turn, is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber."[30]

As discussed below, the FBI requests that certain call identifying features be implemented in a manner PrimeCo submits is *not* cost-effective, as required by statute. Furthermore, these capabilities are not currently provided to law enforcement, and therefore contravene Congress' intent that CALEA standards provide law enforcement "no more and no less access to information than it had in the past."

1. Flash Hook/Feature Keys — Punch List Item 3

FBI/DOJ request that the Commission require carriers to enable law enforcement to receive a data message when the subject of a court order presses a feature or flash hook to hold or transfer a call.[31] FBI/DOJ assert that under the J-Standard, "law enforcement will not receive call-identifying information indicating that the intercept subject has, for example, pressed or dialed certain feature keys to manipulate the call."

---

29 47 U.S.C. § 1002(a)(2). For pen registers and trap and trace devices, however, such call-identifying information may not include information that may disclose the physical location of the subscriber, except to the extent that the location may be determined from the telephone number. *Id.*

30 *Id.* § 1001(2).

31 *See* FBI/DOJ Petition at 36-38, ¶¶ 61-65.

FBI/DOJ further assert that law enforcement has previously had access to such information by detecting recorded changes to the electrical signaling on the analog local loop.[32]

PrimeCo does not address whether the information provided through this feature constitutes call-identifying information.[33] PrimeCo does object, however, to the FBI/DOJ request that this information be provided on a real-time basis. Carriers do not currently provided such information to law enforcement on a real-time basis, so this request contravenes Congress' intent that law enforcement not "require the specific design of systems or features . . . ."[34] Should the Commission determine that this feature provides call-identifying information, a requirement that carriers provide the information to law enforcement *after a call is completed* fully complies with the statutory requirement that carriers provide the information "before, during, *or immediately after* the transmission . . . ."[35] As the J-Standard does not prevent a carrier from providing the information immediately after a call is completed, the J-Standard is CALEA-compliant. Furthermore, given that this information is already available under the J-Standard, requiring carriers to incur additional costs to implement this feature is not cost-effective, again as CALEA requires.

---

32 *Id.* at 36 ¶ 62.

33 PrimeCo notes, however, that CDT asserts that flash hook/feature key signals do not constitute call-identifying information.

34 House Report at 23.

35 *See* 47 U.S.C. § 1002(a)(2)(A) (emphasis added).

2. Post-Cut-Through Dialing — Punch List Item 10

FBI/DOJ request that carriers provide any digits the subject may press after the carrier completes set-up of its portion of the call.[36] The J-Standard, according to FBI/DOJ, denies law enforcement "access to digits dialed after the call is connected."[37] PrimeCo does not address whether the information provided through this feature constitutes call-identifying information.[38] As demonstrated below, however, this feature is "not reasonably available" to the carrier.

As with flash hook/feature keys capability, FBI/DOJ do not tell the whole story regarding post-cut through dialing. First, post-cut through dialing is already provided through a standard Title III call content interception order and existing equipment for law enforcement, such as a JSI Box. PrimeCo's vendor, moreover, has informed PrimeCo that this feature will be extremely costly to develop and, indeed, may be cost prohibitive. For these reasons, the FBI's request this information be delivered to law enforcement via an "InBandsDigit message containing those digits" is unnecessary and hardly "cost effective" as required under CALEA.

3. Information on Participants in a Multi-Party Call — Punch List Item 2

FBI/DOJ request that carriers be required to deliver new data messages, including a "party hold," "party join," and "party drop" messages. According to FBI/DOJ, "exclusion of this information from the interim standard will deprive law

---

36 FBI/DOJ Petition at 39-42, ¶¶ 68-72.

37 *Id.* at 39, ¶ 67.

38 CDT, however, asserts that post-cut through dialing does not constitute call-identifying information. CDT Petition at 13.

enforcement of important investigative and evidentiary information to which it is lawfully entitled." While FBI/DOJ acknowledge that law enforcement did not have access to such information prior to CALEA, they contend that the statutory definition of call identifying information "now obligates carriers to provide this information."[39]

As a threshold matter, imposing this feature on carriers would contravene Congress' admonition that CALEA "provide law enforcement no more and no less access to information than it had in the past" and that law enforcement and the Commission "narrowly interpret the requirements."[40] More fundamentally, FBI/DOJ have misconstrued CALEA's requirements. CALEA's definition of "call identifying information" does just what Congress intended — defines "call identifying information" — and does not obligate carriers to do anything. Rather, it is a separate provision of CALEA — *Section 103(a)* — which requires carriers to provide access to *certain* call identifying information, specifically such information "that is *reasonably available to the carrier.*"[41] Thus, even assuming *arguendo* that this information is deemed call identifying information, FBI/DOJ must demonstrate further that access to such information is reasonably available to the carrier, which it has failed to do. Finally, FBI/DOJ apparently want this information for all participants to a call, regardless of whether the participant was a target of the wiretap. Given CALEA's requirement that the Commission protect the privacy and security of communications not authorized to be intercepted, to the extent that this

---

39 FBI/DOJ Petition at 44, ¶ 77.

40 *See* House Report at 22-23.

41 47 U.S.C. § 1002(a).

capability must be made available to law enforcement, it should be provided only for the target subject invoking the relevant features.

4. Delivery of Call-Identifying Information on a Call Data Channel

FBI/DOJ request that the Commission require carriers to deliver certain call identifying information over a call data channel.[42] While agreeing "that a carrier could comply with its delivery obligations under Section 103 without delivering this information in this fashion," FBI/DOJ contend that CALEA's requirement that industry and government agencies consult with each other "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements under Section 103" provides a statutory basis for requiring this capability.[43]

To start, FBI/DOJ have misread the statute. Section 107(a)(1) goes to the *implementation* of capability requirements. Delivery of call identifying information, however, is a capability requirement in itself, which CALEA requires be accomplished "in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier."[44] Nowhere do FBI/DOJ contend that the J-Standard does not satisfy this requirement, and for this reason alone this request must be rejected.

In addition, FBI/DOJ again are requesting a capability not currently provided to law enforcement and, again, have disregarded Congress' intent that CALEA

---

42 FBI/DOJ Petition at 47-49, ¶¶ 83-85.

43 47 U.S.C. § 1006(a)(1).

44 *Id.* § 1002(a)(3).

"provide law enforcement no more and no less access to information than it had in the past . . . ."[45] This FBI/DOJ request also directly contravenes Congress' admonition that law enforcement "not require the specific design of systems or features" and that "the telecommunications industry itself shall decide how to implement law enforcement's requirements."[46] Finally, law enforcement's existing ability to obtain this information over a voice channel and with a Title III order also calls into question whether this requirement is cost-effective, as required under Section 107(b)(1).

5. Access to Network-Generated Signaling — Punch List Item 4

FBI/DOJ request that the Commission require carriers to deliver network signals including ringing, busy signals, or a call waiting signal.[47] The J-Standard, according to FBI/DOJ, does not require carriers to provide law enforcement with notification of these network-generated call process signals. According to FBI/DOJ, this omission contravenes CALEA's capability requirements because *any* signaling information indicating how the network treated a call attempt purportedly constitutes call identifying information to which carriers must provide access.[48]

FBI/DOJ again ignore the Section 103(a) requirement that carriers provide access to call identifying information "that is *reasonably available to the carrier*." Such information is *already* available via a call content interception and the audio portion of the call. The same equipment that law enforcement uses for pen registers — *e.g.*, a JSI

---

45 House Report at 22-23.

46 *See id.* at 19, 23.

47 FBI/DOJ Petition at 45-46, ¶¶ 80-82.

48 *Id.* at 46, ¶ 81.

Box — already possesses audio capability. All that law enforcement needs to do is obtain a lawful Title III interception order, and switch the audio portion on to listen for ringing and busy tones. Thus, even assuming *arguendo* that this information is call identifying information, law enforcement's existing ability to obtain this information calls into question whether this requirement is cost-effective, as required under Section 107(b)(1).[49] Furthermore, since carriers can provide access to this information without implementing this feature, FBI/DOJ's requested capability conflicts with Congress' intent that Congress "not require the specific design of systems or features" and that "the telecommunications industry itself shall decide how to implement law enforcement's requirements."[50]

C. Timely Delivery of Call-Identifying Information — Punch List Item 5

CALEA requires that carriers be capable of providing law enforcement with access to call-identifying information "before, during, *or immediately after* the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government)."[51] FBI/DOJ request that the Commission require carriers to time-stamp information within 100 milliseconds (one tenth of a second) and that the information be delivered to law enforcement within either three or five seconds.[52] In the next paragraph, however, FBI/DOJ acknowledge that its requested requirements "are not

---

49 *See* 47 U.S.C. § 1006(b)(1).

50 *See* House Report at 19, 23.

51 47 U.S.C. § 1002(a)(2)(A) (emphasis added).

52 FBI/DOJ Petition at 51, ¶ 90.

the only ones that would satisfy" CALEA.[53] PrimeCo submits that CALEA's general "immediately after" requirement, in itself, when combined with the specter of sanctions for noncompliance, provides carriers with sufficient flexibility and incentive to meet law enforcement's legitimate needs.

First, carriers vary considerably in size and technical resources and may utilize a variety of vendors. Thus, a uniform timing standard is not appropriate. In any event, the 3-5 second standard is simply not feasible all the time because of network traffic flows and congestion — much of which occurs outside of PrimeCo's network and over which it has no control.[54] Carriers are subject to significant sanctions for noncompliance with CALEA's capability requirements, which provides ample incentive for carriers to make intercept information available to law enforcement as soon as possible after a call ends.[55] As there is nothing in the J-Standard that would prevent carriers from expeditiously delivering information to law enforcement, and as the information law enforcement desires is readily available after a call ends, the Commission should not adopt a uniform standard for delivery.

---

53 *Id.* at 52, ¶ 93.

54 The Commission has abstained from imposing capability or technical requirements on individual carriers where non-compliance would result from factors beyond the individual carrier's control. *See, e.g., Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, Memorandum Opinion and Order,* CC Docket No. 94-102, FCC 97-402, ¶¶ 106-107 (rel. Dec. 23, 1997) (allowing for waiver of Phase I E-911 where LEC not capable of transmitting ANI information).

55 *See* 18 U.S.C. § 2522.

D. Automated Delivery of Surveillance Status Messages — Punch List Items 6, 7 and 8

The FBI requests that the Commission require carriers to "assure law enforcement that the carrier's equipment is operational" by providing law enforcement three automated status messages:

- A *continuity tone* alerting law enforcement if the facility used for the delivery of call content interception was failed or lost continuity;[56]
- A *surveillance status* message indicating that the interception is working correcting and is accessing the correct service;[57] and
- A *feature status* message notifying law enforcement of any change in a subject's subscribed-to features.[58]

The FBI acknowledges, however, that this proposal is "not the only means by which the requirements of [Section 103] could be satisfied."[59]

FBI/DOJ correctly quote the statute in noting that "Section 103 of CALEA provides that a telecommunications carrier '*shall ensure*' that its equipment is capable of intercepting communications and isolating call-identifying information." In a puzzling leap of statutory interpretation, however, FBI/DOJ next assert that "Section 103 thereby places an affirmative obligation upon the carrier to verify that its equipment is operational and that law enforcement has access to all communications and information within

---

56 FBI/DOJ Petition at 54, ¶ 98.

57 *Id.* at 54-55, ¶¶ 99-100.

58 *Id.* at 56-57, ¶¶ 101-103.

59 *Id.* at 53-54, ¶ 97.

the scope of the authorized surveillance."[60] The Commission should not embrace FBI/DOJ's strained interpretation of CALEA's capability requirements. CALEA's enforcement provisions, which expressly authorize courts to issue enforcement orders, are Congress' intended means of providing that carriers "shall ensure" compliance with the capability requirements.[61]

Furthermore, these requirements are unreasonable and unnecessary. Regarding the "continuity tone" request, FBI/DOJ again would require that a carrier be required to provide capabilities for network equipment other than its own. PrimeCo can only monitor circuit portions residing within its own network, such as switching trunks. If there is a problem with, for example, a T-1 leased by law enforcement and supplied by a LEC, PrimeCo has no control over this network element and cannot reasonably be expected to monitor whether the delivery channels have failed. Furthermore, every circuit has a special tone or idle pattern; if the tone disappears, then the circuit has gone down. Law enforcement can easily detect this idle pattern tone by attaching a pair of readily available MF receivers to, for example, a JSI Box. Regarding surveillance status, a more reasonable means of verifying whether a wiretap is operational is to perform a periodic trap and trace test of the target's phone number to verify that it is working.

Finally, for a feature status message, real-time access and notification of changes in a wiretap subject's service and/or features, the FBI/DOJ request is unnecessary and costly, and more fundamentally, notification of changes in service is not "call identifying information." A carrier's method for service delivery of features has nothing

---

60 *Id.* at 52, ¶ 94.

61 18 U.S.C. §§ 2518(4), 2522.

to do with call-identifying information and such changes should not be subject to law enforcement access on a real-time basis. It can take up to 24 hours between the time a change in features is requested and the time that the change is implemented, and thus real time notification is unnecessary. It should be noted, however, that not all features and services are captured within AMA records, because in some cases, non-billable services will not be captured at all.[62] For those services which are billable and captured in AMA records, law enforcement can be notified within several hours after the change is requested via a customer account activity report. If, however there is a change in features or services outside of PrimeCo's network, PrimeCo's records will not reflect such a change and notification to law enforcement would not be feasible.

E. Standardization of Delivery Interface Protocols — Punch List Item # 8

FBI/DOJ request that the Commission require industry to use "no more than five" delivery interface protocols. It acknowledges, however, that CALEA does "not obligate carriers to use any particular interface protocol," and DOJ separately concluded that this capability is not mandated by CALEA. PrimeCo submits that such a requirement is premature and, in any event, this issue is best left to industry.

---

62 AMA — Automatic Message Accounting — is data provided by the switch for billing purposes and call activity reporting.